REMARKS

Reconsideration of this application is respectfully requested in view of the foregoing amendment and the following remarks.

Claims 1-8, 12-19, 23-30, 33-44, and 47-50 were pending in this application. Claims 1-8 and 12-19 have been cancelled without prejudice or disclaimer to the subject matter thereof. Accordingly, claims 23-30, 33-44, and 47-50 will be pending herein upon entry of this Amendment. For at least the reasons stated below, Applicants respectfully submit that all claims pending in this application are in condition for allowance.

In the Office Action mailed April 7, 2004, claims 1, 2, 5, 7, 8, 12, 13, 16, 18, 19, 23, 24, 27, 29, 30, 37, 38, 41, 43, and 44 were rejected under 35 USC § 102(e) as being anticipated by Munson (US Patent No. 6,681, 331) and claims 3, 4, 6, 14, 15, 17, 25, 26, 28, 39, 40, and 42 were rejected under 35 USC § 103(a) as being unpatentable over Munson, in view of Rowland (US Patent No. 6,405,318), which are addressed below. To the extent these rejections might still be applied to claims presently pending in this application, they are respectfully traversed.

Regarding the anticipation rejection of claims 23 and 37, as previously stated, Applicants note that Munson generally teaches a manner of anomaly detection by comparing events generated on a computer to events deemed to be normal and determining whether the generated event is normal or abnormal, but the specific manner that Munson teaches to determine whether an event is normal or abnormal is quite different from the present invention. The system described in Munson utilizes multinomial distributions to determine abnormality. The present system employs neural networks that have been previously trained to identify normal behavior.

The detected behavior is then analyzed, often in real-time, to determine if that particular data stream is normal.

At least claims 23 and 37 (and by incorporation each of their respective dependent claims) include specific reference to the above-referenced "neural networks", which are not employed, or even discussed in Munson. Examiner's indication of this element being taught at col. 7, lines 17-20, is not equivalent (nor does it even mention) neural networks that are "trained to identify a pre-determined behavior pattern for a corresponding one of the plurality of applications." Nor is data collected via an application profile "sequentially input into a corresponding one of the plurality of neural networks" in order to obtain "a behavior indicator for each of the plurality of data strings in the application profile." In fact, the analysis performed by Munson relates to multinomial statistical analysis of detected events versus known normal events and does not involve the use of neural networks as described in claims 23 and 37. In order for a rejection to be maintained under 35 USC § 102, each and every limitation of the claims must be present in the cited reference. Clearly at least the use of neural networks for intrusion detection as claimed is not taught by Munson.

Further, Applicants claimed "application profiles" are not equivalent to the operational profiles utilized by Munson, as suggested by the Examiner. Munson defines his operational profiles at col. 9, lines 20-25 as "[t]he set of unconditional probabilities of each of the operations in O being executed by the user." Munson then bases its intrusion detection upon these operational profiles by comparing what is occurring in the operational profiles to pre-existing intrusion profiles data (col. 4, lines 26-65). This type of comparison is not what is claimed in claims 23 or 37. Applicants' application profiles "comprise a plurality of application data for a corresponding one of the plurality of applications," and have nothing to do with unconditional probabilities. In fact, the present approach forgoes the computation of probabilities, which often provides for better results than explicitly computing probabilities as is performed in Munson. Next, "a behavior indicator for each of the plurality of data strings in the application profile" is output and "if the behavior indicator meets a pre-determined criteria, a counter is incremented." This is not the same analysis performed in Munson and the Examiner has pointed to no teaching in Munson that could be considered equivalent.

Regarding the rejection based upon the combination of Munson with Bergman et al., such a combination is essentially infeasible. The nodes referred to in Bergman are nodes of the communications network itself, not of a neural network (which as noted above is not even disclosed by Munson). The nodes recited in claims 33-35 and 47-49 reside in the plurality of neural networks. Backpropogation is a learning algorithm utilized in neural networks, there simply is no such thing as backpropogation of a communications network. Further, backpropogation occurs before the neural network is deployed. It is impossible for the backpropogation of a neural network *before* deployment to contain evidence of activity deemed intrusive *after* the network is deployed. Accordingly any combination of Munson with Bergman for the purpose described by the Examiner must fail.

As to Rowland, because this reference is applied only to dependent claims and fails to supply any of the above-cited deficiencies with respect to the Munson reference, Applicants assert that the combination of Rowland and Munson still does not teach each element of the independent claims at issue.

In summation, Applicants do not assert to have invented intrusion detection. Applicants do however, believe the present application represents a novel manner of intrusion detection involving neural networks. While the cited references my involve a type of intrusion detection, it is not the type specifically claimed in either of independent claims 23 or 37 or their associated dependent claims. Applicants have noted several deficiencies in the application of Munson, both alone and in combination with other references. Accordingly, because each element recited in each of the independent claims is not present in either the Munson, Bergman, or Rowland references, Applicants assert that claims 23 and 37 along with their respective dependent claims are in condition for allowance. Should the Examiner have any questions or determine that any further action is desirable to place this application in even better condition for issue, the Examiner is encouraged to telephone applicants' undersigned representative at the number listed below.

PILLSBURY WINTHROP SHAW PITTMAN LLP
1650 Tysons Boulevard
McLean, VA 22102
Tel: 703-770-7900

Respectfully submitted

ANUP K. GHOSH, ET AL.

Date: April 12, 2005

By: Brett C. Martin

Brett C. Martin
Registration No. 52,000

BCM/lrhj

Customer No. 28970